

THE WHITE HOUSE

TOP SECRET/SENSITIVE

November 16, 1977

TS 770248

~~cy#4~~ Ser. B

Series E, Cy 2

Presidential Directive/NSC-24

TO: The Vice President
 The Secretary of State
 The Secretary of Defense
 The Attorney General
 The Secretary of Commerce
 The Director of Central Intelligence
 The Director, Office of Management and Budget
 The Chairman, Joint Chiefs of Staff
 The Director, Office of Science and Technology Policy
 The Administrator, General Services Administration
 The Assistant to the President for Domestic Affairs and Policy

SUBJECT: Telecommunications Protection Policy

1. The President has reviewed the results of the NSC Special Coordination Committee's consideration of the PRM/NSC-22 study and has reached the following conclusions. It is the President's intention that this directive establish a national policy to guide the conduct of USG activities in and related to security of telecommunications.
2. The National Telecommunications Protection Policy shall consist of the following major elements:
 - a. Government classified information relating to national defense and foreign relations shall be transmitted only by secure means.

NSA review completed

TOP SECRET/SENSITIVE/XGDS2

Classified by: Z. Brzezinski

NSC review completed - may be declassified in part

OSD review(s) completed.

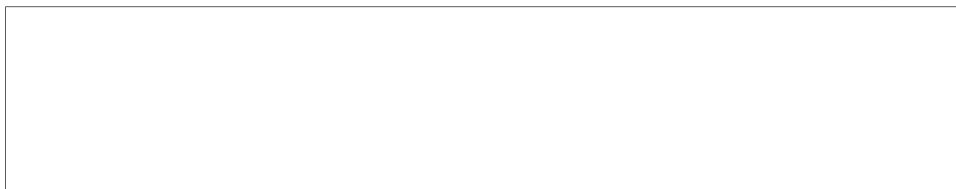
- b. Unclassified information transmitted by and between Government agencies and contractors that would be useful to an adversary should be protected.
 - c. Non-governmental information that would be useful to an adversary shall be identified and the private sector informed of the problem and encouraged to take appropriate protective measures.
 - d. While the private conversations of U.S. citizens do not appear to be the targets of foreign intercept activity at this time, this judgment should be kept under close and continuous review and the American people informed of any change in this conclusion. As a precautionary measure, the responsible Agencies should work with the FCC and the common carriers to adopt system capabilities which protect the privacy of individual communications and to carry out changes in regulatory policy and draft legislation that may be required. Further, the NSC Special Coordination Committee shall periodically review the extent to which the Soviets or others may be collecting and exploiting individual private communications to determine if additional surveillance or protection activity is warranted. Finally, the laws which protect against criminal domestic acts such as wiretaps or intercept shall be strictly enforced.
3. The following activities should be pursued in support of the above policy:
- a. The private sector telecommunications carriers should be briefed on the nature of the threat and appropriate government R&D information shall be made available so as to help and encourage them to devise adequate protection strategies. A similar program shall be pursued for government contractors and other most likely affected industries, corporations and private sector entities.
 - b. The Secretary of Defense shall initiate, through the industrial security mechanism, new and improved personal and telecommunications security measures among business organizations holding classified Defense contracts.
 - c. All departments and agencies shall revitalize programs of security training for U.S. Government personnel who use telephones and other means of communication for both unclassified and classified purposes.
 - d. A permanent interagency group under the chairmanship of the Department of State shall be established consisting of representatives of the Executive Office of the President, the Director of Central

Intelligence, the Department of Defense, the National Security Agency, and the Department of Justice/Federal Bureau of Investigation to review and if necessary to deny real estate acquisitions through lease or purchase by the USSR and other Communist countries that present a serious potential threat to U.S. telecommunications security.

- e. All foreign government leased or owned facilities in this country should be evaluated as to their possible use for intercept operations and appropriate investigative action undertaken in the most likely cases. Any identified intercept activities should be monitored to determine the threat posed to USG and private sector telecommunications.
- f. Subject to continuous review of available technology and reassessment of the foreign intercept threat the following immediate technical actions shall be undertaken:

- The government shall conduct a multi-faceted R&D program covering both system and user oriented protection approaches funded at about \$15 million per year.

-



25X3

- Executive Secure Voice Network (ESVN) systems shall be installed when appropriate high priority requirements can be validated.

- 4. Management and policy review responsibilities for telecommunication protection shall be organized as follows:
 - a. The NSC Special Coordination Committee (SCC) shall be responsible for providing policy guidance and for ensuring full implementation of this directive, including effective protection techniques for the government and maximum assistance to the private sector to enhance its protection from interception. The SCC shall exercise this responsibility through a special Subcommittee on Telecommunications Protection chaired by the Director, Office of Science and Technology Policy, with administrative support provided by the Secretary of Commerce. The Subcommittee shall include but not be limited to representatives of the following departments and agencies: State, Treasury, Justice, Commerce, Defense, Transportation, Energy, Central Intelligence Agency, General Services Administration, the National Security Agency, and the National Security Council Staff.

TOP SECRET/SENSITIVE (

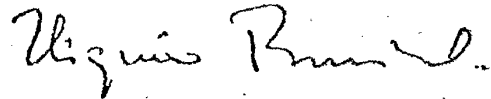
- b. The Subcommittee shall submit a report on its activities, recommendations and findings at least annually to the National Security Council through the Special Coordination Committee. Additionally, that report shall specifically address how effectively the policy and actions specified in this directive are being implemented.
- c. The Secretary of Defense shall act as the Executive Agent for communications security (COMSEC) to protect government-derived classified information and government-derived unclassified information which relates to national security. COMSEC is concerned with protective measures designed for the security of classified information and other information related to national security.
- d. The Secretary of Commerce shall act as the Executive Agent for communications protection for government-derived unclassified information (excluding that relating to national security) and for dealing with the commercial and private sector to enhance their communications protection and privacy.
- e. It is recognized that there will be some overlap between the responsibilities of the Executive Agents in that Defense will continue to provide some non-cryptographic protection for government-derived unclassified information as it does now, and Commerce will have responsibilities in commercial application of cryptographic technology. The Subcommittee will review such areas on a case-by-case basis and attempt to minimize any redundancies.
- f. The Subcommittee should choose a future implementation strategy based on cost-benefit analysis, legal considerations and regulatory policy. As an initial action, the heads of departments and agencies, as designated by the Subcommittee, shall assess the need for protection of unclassified information transmitted under their auspices and report their conclusions to the Subcommittee within 60 days. The Subcommittee shall then set appropriate standards for protection.
- g. The heads of all departments and agencies of the Federal Government shall organize and conduct their communications security and emanations security activities as they see fit subject to the provisions of law, the provisions of this and other applicable directives, and decisions of the Subcommittee. Nothing in this directive shall relieve the

TOP SECRET/SENSITIVE/XGDS2

TOP SECRET/SENSITIVE

heads of the individual departments and agencies of their responsibilities for executing all measures required to assure the security of federal telecommunications and the control of compromising emanations.

- h. The President's Science Advisor, as Chairman of the Subcommittee, shall promptly prepare and arrange for a comprehensive briefing for the Senate and House Select Committees on Intelligence concerning the Administration's new Telecommunications Protection Policy.
5. NSDM's 266, 296, 338 and 346 and the 1968 NSC Communications Security Directive are hereby rescinded.
6. The Office of Management and Budget and the Attorney General are to resolve, as a matter of priority, the necessary arrangements for funding and legal accommodation, to include appropriate legislation, if necessary, to enable expeditious implementation of actions directed above.



Zbigniew Brzezinski

TOP SECRET/SENSITIVE/XGDS2

Page Denied

Next 1 Page(s) In Document Denied

NSC review completed - and takes no action on document